Free Questions for AZ-800 by ebraindumps

Shared by King on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

SIMULATION

Task 10

You use a Group Policy preference to map \\dd.contoso.com\instal1 as drive H for all users. If a user already has an existing drive mapping for H. the new drive mapping must take precedence.

Options:

A- See the solution of this Task below in Explanation

Answer:

A

Explanation:

To map\\dd.contoso.com\instal1as drive H for all users using Group Policy Preferences and ensure that the new drive mapping takes precedence over any existing mappings, follow these steps:

Step 1: Open Group Policy Management ConsoleOpen the Group Policy Management Console (GPMC) on a machine that has administrative privileges over the domain.

Step 2: Create or Edit a GPOCreate a new Group Policy Object (GPO) or edit an existing one that applies to the users who need the drive mapping.

Step 3: Navigate to Drive MappingsIn the GPO Editor, navigate to:

User Configuration -> Preferences -> Windows Settings -> Drive Maps

Step 4: New Drive MappingRight-click on Drive Maps and selectNew->Mapped Drive.

Step 5: Configure Drive MappingIn the New Drive Properties window, configure the following settings:

Action: SelectReplace. This action will overwrite any existing mappings with the same drive letter.

Location: Enter the UNC path\\dd.contoso.com\instal1.

Drive Letter: ChooseH:from the drop-down menu.

Reconnect: Check this option if you want the drive mapping to persist across logon sessions.

Label As: Optionally, provide a label for the drive mapping.

Hide/Show this drive: Set according to your preference.

Hide/Show all drives: Set according to your preference.

Step 6: Common TabGo to theCommontab and configure the following:

Run in logged-on user's security context (user policy option): Check this option.

Item-level targeting: Click onTargetingand set up any specific criteria if needed.

Step 7: Apply the GPOClickApplyand thenOKto save the drive mapping configuration.

Step 8: Link the GPOLink the GPO to an Organizational Unit (OU) or domain that contains the users who should receive the drive mapping.

Step 9: Update Group PolicyInstruct users to log off and log back on, or use thegpupdate /forcecommand to refresh Group Policy on their computers.

Question 2

Question Type: **MultipleChoice**

SIMULATION

Task 9

You need to ensure that all the computers in the domain use DNSSEC to resolve names in the adatum.com zone.

Options:

A- See the solution of this Task below in Explanation

Answer:

A

Explanation:

To ensure that all computers in the domain use DNSSEC to resolve names in the adatum.com zone, you'll need to configure both the DNS servers and the client computers. Here's how you can do it:

Step 1: Sign the adatum.com Zone First, you need to sign the adatum.com DNS zone. This can be done using the DNS Manager or PowerShell. Here's a PowerShell example:

Add-DnsServerSigningKey -ZoneName 'adatum.com' -CryptoAlgorithm RsaSha256

Set-DnsServerDnsSecZoneSetting -ZoneName 'adatum.com' -DenialOfExistence NSEC3 -NSEC3Parameters 1,0,10,''

This will add a signing key and configure DNSSEC for the zone with NSEC3 parameters.

Step 2: Configure DNS Servers Ensure that your DNS servers are configured to support DNSSEC. This includes setting up trust anchors for the zones that you want to validate and configuring the DNS servers to provide DNSSEC validation for DNS queries.

Step 3: Configure DNS Clients For DNSSEC validation to occur on the client side, the client computers must be configured to trust the DNS server's validation process. This typically involves configuring the client's DNS settings to point to a DNS server that supports DNSSEC.

Step 4: Validate Configuration You can validate that DNSSEC is working correctly by using tools like nslookup or dig to query DNS records and check for the presence of DNSSEC signatures in the responses.

Note: The exact steps may vary depending on your environment and the version of Windows Server you are using. Ensure that you have the appropriate administrative rights to make these changes and that you test the configuration in a controlled environment before deploying it domain-wide12.

By following these steps, you should be able to ensure that all computers in your domain use DNSSEC to resolve names in the adatum.com zone.

Question 3

Question Type: **MultipleChoice**

SIMULATION

Task 8

You need to deploy a new primary DNS zone named fabrikam.com to DC1. The zone must be signed.

Options:

A- See the solution of this Task below in Explanation

Answer:

A

Explanation:

To deploy a new primary DNS zone named fabrikam.com to DC1 and sign the zone, you can follow these steps:

Step 1: Create the Primary DNS Zone Use the Add-DnsServerPrimaryZone PowerShell command to create the primary zone:

Add-DnsServerPrimaryZone -Name 'fabrikam.com' -ZoneFile 'fabrikam.com.dns' -DynamicUpdate Secure

This command creates a primary zone for fabrikam.com with a DNS file named fabrikam.com.dns and allows secure dynamic updates.

Step 2: Sign the Zone To sign the zone, you can use the DNS Manager or Windows PowerShell. Here's how to sign the zone using PowerShell:

Add-DnsServerSigningKey -ZoneName 'fabrikam.com' -Type KeySigningKey -CryptoAlgorithm RsaSha256

Set-DnsServerDnsSecZoneSetting -ZoneName 'fabrikam.com' -DenialOfExistence NSEC3 -NSEC3Parameters 1,0,10,''

These commands add a signing key to the zone and set DNSSEC settings with NSEC3 parameters.

Step 3: Publish the Signed Zone After signing the zone, ensure that it is published and available for DNS queries. You can verify the zone signing status using the following command:

Get-DnsServerZone -Name 'fabrikam.com'

Note: Ensure that you have the appropriate permissions to perform these actions on DC1 and that the DNS Server role is installed and properly configured. Also, replace 'fabrikam.com.dns' with the actual path to your DNS file if it's different12.

By following these steps, you should be able to deploy and sign the new primary DNS zone fabrikam.com on DC1.

Question 4

Question Type: **MultipleChoice**

SIMULATION

Task 7

You need to collect the recommended Windows Performance Counters from SRV1 in a Log Analytics workspace.

The required tiles are stored in a shared folder named \dc\install.

Options:

A- See the solution of this Task below in Explanation

Answer:

A

Explanation:

To collect the recommended Windows Performance Counters from SRV1 in a Log Analytics workspace, you can follow these steps:

Step 1: Access the Log Analytics Workspace Log in to the Azure portal and navigate to your Log Analytics workspace.

Step 2: Configure Performance Counters In the Log Analytics workspace, select Advanced settings and then choose Data > Windows Performance Counters1. You can add the recommended performance counters by selecting the + button. If you're using legacy agent management, you can add counters from the Legacy agents management menu2.

Step 3: Add Performance Counters Select the counters you want to collect. You can add common counters quickly by checking the boxes next to them. For specific counters, enter the name of the counter in the format object(instance)\counter. For example, to collect the Processor Time counter for all instances of the Processor object, specify Processor(_Total)\% Processor Time.

Step 4: Set Sample Interval When adding a counter, you can set the sample interval, which is the frequency at which data is collected. The default is 10 seconds, but you can change this to a higher value if needed.

Step 5: Apply Configuration After adding the desired performance counters, select Apply at the top of the screen to save the configuration.

Step 6: Install and Configure the Agent Ensure that the Microsoft Monitoring Agent (MMA) is installed on SRV1. Configure the agent to report to your Log Analytics workspace by specifying the workspace ID and key during setup.

Step 7: Verify Data Collection After the agent is configured, it will start collecting the specified performance counters. You can verify the data collection in the Log Analytics workspace by running queries against the collected data.

Note: The legacy Log Analytics agent will be deprecated by August 2024. Migrate to the Azure Monitor agent before this date to continue ingesting data3.

By following these steps, you should be able to collect the recommended Windows Performance Counters from SRV1 in your Log Analytics workspace. Ensure that you have the necessary permissions and that SRV1 has network connectivity to Azure services.

Question 5

Question Type: **MultipleChoice**

SIMULATION

Task 6

You need to use Azure File Sync 10 replicate the contents of C:\app on SRV1 to an Azure file share named sharel1.

The required source files are located in a folder named \\dc1.contoso.com\install.

Options:

A- See the solution of this Task below in Explanation

Answer:

A

Explanation:

To use Azure File Sync to replicate the contents of C:\app on SRV1 to an Azure file share named sharel1, with the source files located in \\dc1.contoso.com\install, follow these steps:

Step 1: Prepare Windows Server for Azure File Sync Ensure that SRV1 meets the prerequisites for Azure File Sync, such as having a supported version of Windows Server and PowerShell 5.1 or later1.

Step 2: Deploy the Storage Sync Service In the Azure portal, deploy the Storage Sync Service in the same region as your Azure file share1.

Step 3: Create an Azure File Share Create an Azure file share named sharel1 in your storage account1.

Step 4: Install the Azure File Sync Agent Download and install the Azure File Sync agent on SRV11.

Step 5: Register SRV1 with the Storage Sync Service After installing the agent, register SRV1 with the Storage Sync Service using the Azure portal1.

Step 6: Create a Sync Group and Server Endpoint In the Azure portal, go to your Storage Sync Service and create a new sync group. Add a server endpoint with the path C:\app on SRV12.

Step 7: Configure Cloud Endpoint Add the Azure file share sharel1 as the cloud endpoint to the sync group2.

Step 8: Initiate the Sync Process The initial sync will start automatically after the cloud endpoint and server endpoint are added to the sync group. Ensure that the Azure File Sync agent is running on SRV11.

Step 9: Monitor the Sync Status Monitor the sync status in the Azure portal to ensure that the files are being replicated correctly from C:\app on SRV1 to the Azure file share sharel11.

Note: Make sure that the network connectivity between SRV1 and the Azure file share is established and that the necessary ports are open. Also, verify that the SMB security settings allow for the required SMB protocol version and authentication methods1.

By following these steps, you should be able to replicate the contents of C:\app on SRV1 to the Azure file share sharel1 using Azure File Sync. Ensure that you have the necessary permissions to perform these actions and that SRV1 is properly configured to communicate with Azure services.

Question 6

Question Type: **MultipleChoice**

SIMULATION

Task 5

You have an application that is copied to a folder named C:\app on SRV1. C:\app also contains also a Dockerfile for the app.

On SRV1. you need to create a container image for the application by using the Dockerfile. The container image mutt be named app1.

Options:

A- See the solution of this Task below in Explanation

Answer:

A

Explanation:

Explore

To create a container image named app1 for your application using the Dockerfile in the C:\app directory on SRV1, follow these steps:

Step 1: Open PowerShell or Command Prompt First, open PowerShell or Command Prompt on SRV1.

Step 2: Navigate to the Application Directory Change to the directory where your application and Dockerfile are located:

cd C:\app

Step 3: Build the Container Image Use the docker build command to create the container image. The -t flag tags the image with the name app1:

docker build -t app1 .

The period . at the end of the command tells Docker to use the Dockerfile in the current directory.

Step 4: Verify the Image Creation After the build process completes, verify that the image app1 has been created successfully by listing all images:

docker images

You should see app1 in the list of images.

Step 5: Use the Image Now, you can use the image app1 to run containers or push it to a container registry if needed.

By following these steps, you'll have created a Docker container image named app1 using the Dockerfile located in C:\app on SRV11. Ensure that Docker is installed on SRV1 and that you have the necessary permissions to execute these commands.